xahive

Your Cybersecurity Partner

XAHIVE's CYBERSECURITY INCIDENT CHECKLIST

BEFORE AN INCIDENT

 Create a prioritized list of information assets critical to the functioning of your organization.

 Identify the stakeholders responsible for each critical asset.

 Create an Incident Response Team, who will be responsible for all incidents (including individuals from legal, corporate communications, and HR).

 Ensure proper monitoring and tracking technologies are in place to protect your organization's information assets (such as firewalls, IPS, and anti-virus).

 Provide media training to the proper individual(s).

 Provide a company-wide process for employees, contractors, and third parties to report suspicious or suspected breach activities.

 Provide company-wide training on breach awareness, employee responsibility, and reporting processes.

DURING AN INCIDENT

 Record the issues and open an incident report.

 Convene the Incident Response Team.

 Convene a teleconference with requisite stakeholders to discuss what must be done in order to restore operations.

 Convene a management teleconference with requisite stakeholders in order to provide situational awareness to executive management.

 Triage the current issues and communicate to executive management.

 Identify the initial cause of the incident and activate the specialists to respond to the current issues to restore operations.

 Retain any evidence and follow a strict chain of evidence to support any needed or anticipated legal action.

 Communicate to affected third parties, regulators, and media (if appropriate).

(U.S.) Main Office & Mailing Address: 347 Fifth Avenue, Suite 1402-285. New York, New York, 10016, USA
(U.S.) 2nd Office Location: 326 Broad Street, Utica, New York 13501, USA
(Canada) Mailing Address: PO BOX # 47056. 2638 Innes Road. Ottawa, Ontario. K1B5P9 CANADA
(Canada) Office Address: 255 Centrum Blvd., Suite 102, Ottawa, ON, K1E 3W3 CANADA
T: 646-205-2246 **T2:** 613-286-6484 **URL:** www.XAHIVE.com, **Email:** sem@XAHIVE.com

xahive

Your Cybersecurity Partner

AFTER AN INCIDENT

 Update the incident report and review exactly what happened and at what times.

 Review how well the staff and management performed in during the incident.

 Determine whether or not the documented procedures were followed.

 Discuss any changes in process or technology that are needed to mitigate future incidents.

 Determine what information was needed sooner.

 Discuss whether any steps or actions taken might have inhibited the recovery.

 Determine which additional tools or resources are needed to detect, triage, analyze, and mitigate future incidents.

 Discuss what reporting requirements are needed (such as regulatory and customer).

 If possible, quantify the financial loss caused by the breach.

(U.S.) Main Office & Mailing Address: 347 Fifth Avenue, Suite 1402-285. New York, New York, 10016, USA
(U.S.) 2nd Office Location: 326 Broad Street, Utica, New York 13501, USA
(Canada) Mailing Address: PO BOX # 47056. 2638 Innes Road. Ottawa, Ontario. K1B5P9 CANADA
(Canada) Office Address: 255 Centrum Blvd., Suite 102, Ottawa, ON, K1E 3W3 CANADA
T: 646-205-2246 **T2:** 613-286-6484 **URL:** www.XAHIVE.com, **Email:** sem@XAHIVE.com